

---

# **HIT Standards Committee Privacy and Security Workgroup**

**Task Update: Standards and Certification Criteria  
for Certifying EHR Modules**

**Dixie Baker, Chair  
Walter Suarez, Co-Chair**

**November 13, 2012**

# Privacy and Security Workgroup

---

- Dixie Baker, SAIC
- John Blair, Taconic IPA
- [Tonya Dorsey, BlueCross BlueShield of South Carolina](#)
- Mike Davis, Veterans Health Administration
- Lisa Gallagher, HIMSS
- [Leslie Kelly-Hall, Healthwise](#)
- Chad Hirsch, Mayo
- Jeff Jonas, IBM
- [Peter Kaufman, DrFirst](#)
- Ed Larsen
- David McCallie, Cerner Corporation
- John Moehrke, General Electric
- Wes Rishel, Gartner
- Kevin Stine, NIST
- Walter Suarez, Kaiser Permanente
- Sharon Terry, Genetic Alliance

## Task Context

---

- 2010 Edition of EHR Certification Program introduced certification of “Complete EHRs” and “EHR Modules”
  - **EHR Modules were certified against all privacy and security criteria**
- 2014 Edition introduced changes aimed at streamlining the certification process and reducing regulatory burden
  - **Eliminated the requirement for EHR Modules to be certified to the privacy and security certification criteria**
  - Introduced “Base EHR definition” – a set of core attributes, including privacy and security, that each Certified EHR Technology (CEHRT) adopted by an eligible professional (EP), eligible hospital (EH), or critical access hospital (CAH) must meet
- Might the pendulum have swung too far? For the 2016 Edition, might it be possible to require that each EHR Module be certified against some minimal set of privacy and security criteria, without imposing unreasonable regulatory burden?

# 2014 Edition: Base EHR Definition

**Table 6. Certification Criteria Required to Satisfy the Base EHR Definition**

EHR technology that:	Certification Criteria
Includes patient demographic and clinical health information, such as medical history and problem lists	Demographics § 170.314(a)(3) Problem List § 170.314(a)(5) Medication List § 170.314(a)(6) Medication Allergy List § 170.314(a)(7)
Has the capacity to provide clinical decision support	Clinical Decision Support § 170.314(a)(8)
Has the capacity to support physician order entry	Computerized Provider Order Entry § 170.314(a)(1)
Has the capacity to capture and query information relevant to health care quality	Clinical Quality Measures § 170.314(c)(1) through (3)
Has the capacity to exchange electronic health information with, and integrate such information from other sources	Transitions of Care § 170.314(b)(1) and (2) Data Portability § 170.314(b)(7)
Has the capacity to protect the confidentiality, integrity, and availability of health information stored and exchanged	Privacy and Security § 170.314(d)(1) through (8)

# 2014 Privacy and Security Certification Criteria and Related Standards

<b>§170.314 2014 Edition electronic health record certification criteria - (d) Privacy and Security</b>	<b>§170. 210 Standards Adopted</b>
<b>1. Authentication, access control, and authorization</b>	N/A
<b>2. Auditable events and tamper-resistance</b>	Record a defined set of general actions related to electronic health information
<b>3. Audit report(s)</b>	Record a defined set of specific actions related to electronic health information, audit log status, and encryption of end user devices  Synchronized clocks based on Request for Comments (RFC)1305 Network Time Protocol (NTP) v3 or RFC 5905 NTPv4
<b>4. Amendments</b>	N/A
<b>5. Automatic log-off</b>	N/A
<b>6. Emergency access</b>	N/A
<b>7. Encryption of data at rest</b>	Any encryption and hashing algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2
<b>8. Integrity</b>	A hashing algorithm with a security strength equal to or greater than SHA-1
<b>9. Optional-accounting of disclosures</b>	Record certain defined elements related to treatment, payment, and health care operations disclosure

# Task Assignment

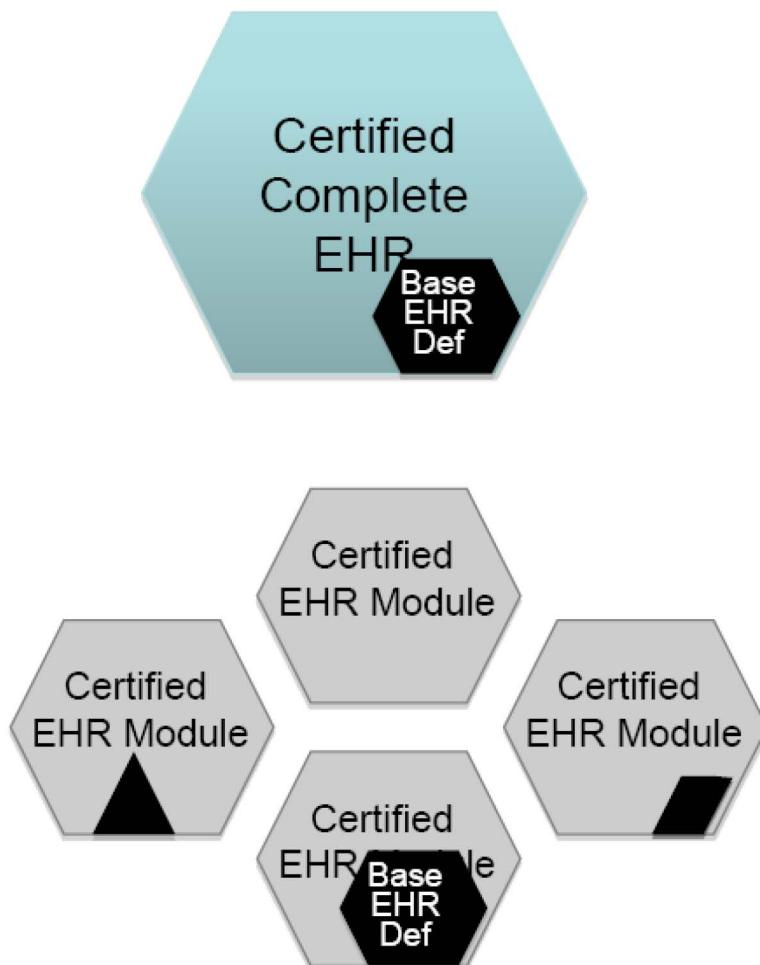
---

- Provide recommendations for certifying EHR Modules under the 2016 Edition of the EHR Certification Program.
  - Identify the minimal set of privacy and security standards and certification criteria
  - Anticipate future broad adoption of NSTIC-based authentication, and therefore should be compatible with the NSTIC\* approach

\*National Strategy for Trusted Identities in Cyberspace

# 2014 Edition: Certification and Adoption

## ONC HIT Certification Program



EPs, EHs, and CAHs are required to meet CEHRT definition by adopting a certified Complete EHR or a combination of certified EHR Modules that together meet the Base EHR definition

*CEHRT is the technology that is implemented in the operational environments of meaningful users*

*This is where HIPAA Privacy and Security Requirements are applied*

# Draft Recommendation – work in progress

- For the 2016 Edition, we recommend that each EHR Module presented for certification be required to meet each privacy and security certification criterion in the minimal set, using one of the following three certification paths:
  1. Demonstrate, through system documentation and certification testing, that the EHR Module includes functionality that fully conforms to the privacy and security certification criterion.
  2. Demonstrate, through system documentation and certification testing, that the EHR Module has implemented standards-based service interfaces that enable it to access external services necessary to conform to the privacy and security certification criterion. [P&S WG will recommend standards for service interfaces]
  3. Demonstrate through documentation that the privacy and security certification criterion is inapplicable or would be technically infeasible for the EHR Module to meet.

# Draft Recommendation – work in progress

- For the 2016 Edition, we recommend that each EHR Module presented for certification be required to meet each privacy and security certification criterion in the minimal set, using one of the following three certification paths:
  1. Demonstrate, through system documentation and certification testing, that the EHR Module includes functionality that fully conforms to the privacy and security certification criterion.
  2. Demonstrate, through system documentation and certification testing, that the EHR Module has implemented standards-based service interfaces that enable it to access external services necessary to conform to the privacy and security certification criterion. [P&S WG will recommend standards for service interfaces]
  3. Demonstrate through system documentation that the EHR Module has implemented non-standards-based service interfaces that enable it to access services provided by other certified EHR technology to conform to the privacy and security certification criterion.
  4. Demonstrate through documentation that the privacy and security certification criterion is inapplicable or would be technically infeasible for the EHR Module to meet.

## Draft Recommendations – Minimal Set

---

- What is the “minimal set” of security functionality that every EHR Module should be required to address via one of the defined paths?
  1. Authentication, access control, and authorization
  2. Auditable events and tamper resistance
  3. Audit report(s)
  4. ~~Amendments~~
  5. Automatic log-off
  6. Emergency access
  7. Encryption of data at rest
  8. Integrity
  9. ~~Optional – accounting of disclosures~~

## Next Steps

---

- Agree upon 3 or 4 paths
- Select interoperability standards
- Solicit public comments through ONC blog
- Present final recommendation to HITSC